PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant:	**Michael John Wray**	Examiner:	Nicole M. Young
Serial No.:	**10/810,308**	Art Unit:	2139
Filed:	03/26/2004	Our Ref:	B-5404 621794-8 30011222-3 US
For:	"SECURITY ATTRIBUTES IN TRUSTED COMPUTING..."	Date:	May 5, 2008
		Re:	***Appeal to the Board of Appeals***

BRIEF ON APPEAL

Sir:

This is an appeal from the Final rejection dated December 5, 2007, for the above identified patent application. Please charge the amount of $510.00 for the fee set forth in 37 C.F.R. 41.20(b)(2) for submitting this Brief to deposit account no. 08-2025. The Appellant submits that this Appeal Brief is being timely filed because the Notice of Appeal was filed on March 5, 2008.

REAL PARTY IN INTEREST

The real party in interest to the present application is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences related to the present application.

STATUS OF CLAIMS

Claims 1-17 were filed with this application. Claims 14 and 17 were cancelled in a preliminary amendment filed on March 26, 2004 (i.e. concurrently with the filing of the application). Claims 1-13, 15, and 16 are the subject of this Appeal and are reproduced in the accompanying appendix. Claim 8 was initially rejected as indefinite, however the Advisory Action of March 25, 2008, removed the indefiniteness rejection and asserting a rejection of obviousness in line with the rejection of claims 1-7, 9-13, 15, and 16 (by stating that it "does not overcome the prior art of record").

STATUS OF AMENDMENTS

An Amendment After Final Rejection has been entered and the amendments therein were accepted by the Examiner, as reported by the Advisory Action of March 25, 2008. The amendments were made to place the application in better form for this appeal: namely, amending the specification to remove a hyperlink reference and amending claim 8 to overcome an indefiniteness rejection.

SUMMARY OF CLAIMED SUBJECT MATTER

The invention described and claimed in claim 1 is directed to a system comprising a trusted computing platform (10) and one or more logically protected computing environments (15), each of which is associated with at least one service or process (15) supported by said system (page 6, paragraph 3, lines 9-11; Figure 1), the system being arranged to load (100) an operating system into said trusted computing platform (10)(page 8, paragraph 3, lines 1-2; Figure 3) and thereafter to load (102) onto said trusted computing platform data defining a predetermined security policy defining security attributes to be applied to one or more of the at least one service or process when said service or process is started (106) (page 8, paragraph 4, line 1, to page 9, paragraph 1, line 2; Figure 3) .

The invention described and claimed in claim 15 is directed to a method of applying a security policy (102) in a system including a trusted computing platform (10) and one or more logically protected computing environments (15), each of which is associated with at least one service or process (15) supported by said system, the method including the steps of loading (100) an operating system into said trusted computing platform (10)(page 8, paragraph 3, lines 9-11;

Figure 3); after loading the operating system, starting (106) a service or process (15) associated with at least one of the logically protected computing environments; and controlling (112) the operation of the at least one logically protected environment by applying, upon starting of the service or process, security attributes to the service or process (page 8, paragraph 4 line 1, to page 9, paragraph 1, line 2; Figure 3).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Issue 1: Whether claims 1-13, 15, and 16 are patentable under 35 U.S.C. 103 over U.S. Patent No. 7,216,369 to Wiseman et al. (hereinafter "Wiseman").

THE ARGUMENT

Issue 1: Whether claims 1-13, 15, and 16 are patentable under 35 U.S.C. 103 over Wiseman.

On page 4 of the Office Action of December 5, 2007, the Examiner rejects claims 1-7, 9-13, 15, and 16 as being obvious over Wiseman. In particular, the Examiner finds that,

> "Wiseman does not teach the Operating System is loaded before the 'data defining a predetermined security policy is loaded'. It would have been obvious to one of ordinary skill in the art at the time the invention was made to rearrange the order of OS and the security (the TPM) when the computer boots. Reversing when the TPM and the OS start does not modify the operation of the device." (office action, page 5)

MPEP 2142 states that in establishing a *prima facie* case of obviousness "The Federal Circuit has stated that "rejections on obviousness cannot be sustained with mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *In re Kahn*, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006)". The Supreme Court in KSR agreed, directly quoting the above statement from *In re Kahn* (*KSR v. Teleflex*, slip op. at p. 14). In this case, the Examiner merely offers the conclusory statements "It would have been obvious … to rearrange the order…" and "Reversing when the TPM and the OS start does not modify…" without giving any articulated reasoning to

support those statements. Therefore, the Examiner has failed to establish a *prima facie* case of obviousness against these claims.

The present application addresses the importance of the distinction between art like Wiseman and the claimed invention, stating in paragraph 4 of page 2 "In the past, it has been considered desirable to load the security rules as early in the startup sequence of a platform as possible, such that relevant security rules are in force as soon as a service or process is started. As such, in prior art systems, all security rules tend to be loaded at system startup. Thus, security attributes tend to be assigned by security initialization and cannot be changed except by processes with special authorization." This description of the prior art also describes Wiseman, because the security policy of Wiseman is a "platform security property policy module...[which] may be included in the PIBB" (Wiseman, col. 3, ll. 47-49) wherein the PIBB is such that "it is assumed that an unauthorized entity will not be able to modify the PIBB" (Wiseman, col. 3, ll. 20-21). Therefore, Wiseman teaches the art that the present application improves upon, not merely a modification of the claimed invention.

Wiseman teaches away from rearranging the order of loading the OS and the security policy. Every example given in Wiseman has the security policy loaded prior to the OS. "Thus, various embodiments of the invention may act to prevent loading of the OS" (col. 3, ll. 25-26), "The comparison module may operate to prevent transfer of control to the OS process" (col. 4, ll.19-20), "if at any time during initialization of the platform a component within the platform violates a policy in the verified platform security property policy module" (col. 4, ll. 24-26), "before transferring control of the platform to the OS Loader, the Main Platform Initialization Code compares the overall configuration and load sequence of the platform by checking the policy table" (col. 4, ll. 63-66), "Typically, the comparison module operates to prevent transfer of control to the operating system...when a policy included in the platform security policy module is violated" (col. 6, ll. 30-34). The Background Information section of Wiseman (col. 1) is primarily focused on the loading of the operating system and pre-operating system components. Figure 3B of Wiseman shows "OS Loader loads OS and transfers control of platform to OS" as being the final step (reference 369) of the flowchart. Given the above facts, one skilled in the art using Wiseman as a guide would not be motivated to "*load an operating system into said trusted computing platform and thereafter to load onto said trusted computing*

platform data defining a predetermined security policy" (claim 1) or "*after loading the operating system, starting a service or process associated with at least one of the logically protected computing environments; and controlling the operation of the at least one logically protected environment by applying, upon starting of the service or process, security attributes to the service or process*" (claim 15) because the reference teaches away from loading in the order recited in the claims.

Further, changing the order of loading would modify the operation of the device of Wiseman (*see* MPEP 2143.01 V. "The Proposed Modification Cannot Render the Prior Art Unsatisfactory for its Intended Purpose" and VI. "The Proposed Modification Cannot Change the Principle of Operation of a Reference"). The abstract of Wiseman states "The comparison module may operate to prevent transfer of control to an operating system (and/or halt the boot process) if a policy included in the platform security property policy is violated." This is only possible if the security property policy is loaded before the operating system is loaded (i.e. "booted"). If the operating system were to be loaded before the policy is installed, then the system would not have a policy to check against to stop the loading of the operating system. Therefore, one skilled in the art using Wiseman as a guide would not be motivated to "*load an operating system into said trusted computing platform and thereafter to load onto said trusted computing platform data defining a predetermined security policy*" (claim 1) or "*after loading the operating system, starting a service or process associated with at least one of the logically protected computing environments; and controlling the operation of the at least one logically protected environment by applying, upon starting of the service or process, security attributes to the service or process*" (claim 15), because doing so would render Wiseman unsatisfactory for its intended purpose of interrupting the OS loading process upon policy violation.

In view of all of the preceding, the Appellant respectfully submits that claims 1 and 8 are in fact patentable over the art on record, and respectfully request that the Examiner be overturned on Appeal and this claim passed to issue.

Claims 2-13 are dependent on claim 1. Therefore, in light of the above discussion of claim 1, the Appellant respectfully submits that claims 2-13 are also allowable at least in view of their dependency on claim 1.

Claim 16 is dependent on claim 15. Therefore, in light of the above discussion of claim 15, the Appellant respectfully submits that claim 16 is also allowable at least in view of its dependency on claim 15.

CONCLUSION

In view of the extensive reasons advanced above, the Appellant respectfully contends that each pending claim is in fact novel and patentable. Therefore, reversal of all rejections and objections and re-opening of the prosecution is respectfully solicited.

I hereby certify that this correspondence is being electronically transmitted via EFS on

May 5, 2008
(Date of Transmission)

Lucy Derby
(Name of Person Transmitting)

(Signature)

5-5-08
(Date)

Respectfully submitted,

Brian J. Cash
Attorney for Appellant
Reg. No. 60,546
LADAS & PARRY
5670 Wilshire Boulevard, Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile
bcash@la.ladas.com

Attachments:
Claims Appendix
Evidence Appendix
Related Proceedings Appendix

Claims Appendix

Claims

1. A system comprising a trusted computing platform and one or more logically protected computing environments, each of which is associated with at least one service or process supported by said system, the system being arranged to load an operating system into said trusted computing platform and thereafter to load onto said trusted computing platform data defining a predetermined security policy defining security attributes to be applied to one or more of the at least one service or process when said service or process is started.

2. A system according to claim 1 wherein the policy included one or more security rules for controlling operation of logically protected computing environments.

3. A system according to claim 2 wherein at least one of the one or more security rules is for at least one of the logically protected environments and includes an execution control rule which defines the security attributes.

4. A system according to claim 3, wherein said security attributes include or comprise one or more capabilities to be provided to the respective logically protected computing environment when said service or process is started.

5. A system according to claim 3, wherein said security attributes include or comprise one or more functions which change or modify the capabilities of the respective logically protected computing environment when said service or process is started.

6. A system according to claim 3, wherein when a service or process is started said security attribute operates to cause the service or process to be placed and run in a specified logically protected computing environment.

7. A system according to claim 3, wherein said security attributes operate to modify a user id, a group id or a logically protected computing environment in which a service or process is to be run.

8. A system according to claim 3, wherein said security attributes operate to change the root directory of the service or process.

9. A system according to claim 5, wherein said execution control rule can raise or lower a specified capability.

10. A system according to claim 5, wherein the security attributes operate to filter a set of capabilities of a logically protected computing environment and modifying only one or more of said capabilities as selected by said filtering means.

11. A system according to claim 3, wherein said execution control rule specifies the service or process to which it applies by identifying the associated logically protected computing environment, with the effect that said rule applies only to services or processes specifying that logically protected computing environment.

12. A system according to claim 3, wherein the files making up a service or process to which said execution control rule applies are of read-only configuration.

13. A system according to claim 3, including means for monitoring operations performed by the system which modify names of files making up services or programs to which said execution control rule applies.

Claim 14. Canceled.

15. A method of applying a security policy in a system including a trusted computing platform and one or more logically protected computing environments, each of which is associated with at least one service or process supported by said system, the method including the steps of loading

an operating system into said trusted computing platform; after loading the operating system, starting a service or process associated with at least one of the logically protected computing environments; and controlling the operation of the at least one logically protected environment by applying, upon starting of the service or process, security attributes to the service or process.

16. A method according to claim 15 wherein the attributes are defined by execution control rules, which are included in security rules implementing at least part of the policy.

Claim 17. Canceled.

Evidence Appendix

There is no evidence submitted with the present Brief on Appeal.

Related Proceedings Appendix

There are no other appeals or interferences related to the present application.